97

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,412	12/21/2001	Alex J. Hinchliffe	002114.P030	3596

8791 7590 03/02/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
DENNISON, JERRY B	
ART UNIT	**PAPER NUMBER**
2143	

DATE MAILED: 03/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/028,412	HINCHLIFFE ET AL.	
	Examiner	Art Unit	
	J. Bret Dennison	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 10/15/02
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Action is in response to Application Number 10/028,412 received on 21 December 2001.

2. Claims 1-44 are presented for examination.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 3, 17, and 31 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. Claims 3, 17, and 31 recite the limitation, "evaluating a change in shared data on a peer". It is unclear to Examiner if this limitation means. Examiner will interpret the limitation as "evaluating changes in the traffic received from the peer". Appropriate correction is required.

Examiner's Interpretation

4. Before a detailed rejection, a brief interpretation of peer-to-peer networks should be discussed. A peer-to-peer network is a communications network in which each party has the same capabilities and either party can initiate a communication session. Peer-to-peer communication may be implemented in a client/server environment by giving each communication node, server and client, the same capabilities, meaning a client can be configured as a server and a server can be configured as a client, where traffic is running in both directions. Monitoring traffic on a peer-to-peer network is the same as

monitoring traffic in both directions on any network. Also, at any one given time you have a client process and a server process, which makes it irrelevant to the type of network being used.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-44 are rejected under 35 U.S.C. 102(e) as being anticipated by Lowell (U.S. Patent Number 6,381,632).

5. Regarding claims 1, 15, and 29, Lowell discloses a computerized method comprising:

monitoring a peer-to-peer network for suspicious activity based on patterns of activity (Lowell, col. 2, lines 45-60); and

performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network (Lowell, col. 2, lines 50-60)

Claims 15 and 29 include a computer-readable medium and system performing the same functionality as claim 1 and are therefore are rejected under the same prior art as being substantially similar.

Claims 1-44 are rejected under 35 U.S.C. 102(e) as being anticipated by Conklin et al. (U.S. Patent Number 5,991,881).

6. Regarding claims 1, 15, and 29, Conklin discloses a computerized method comprising:

monitoring a peer-to-peer network for suspicious activity based on patterns of activity (Conklin, col. 1, lines 10-15, col. 1, line 65 through col. 2, line 5, see Abstract, Conklin discloses monitoring ALL traffic on the network for suspicious activity); and

performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network (Conklin, col. 4, lines 45-55, Conklin discloses performing actions associated with a particular pattern)

Claims 15 and 29 include a computer-readable medium and system performing the same functionality as claim 1 and are therefore are rejected under the same prior art as being substantially similar.

Claims 1-44 are rejected under 35 U.S.C. 102(e) as being anticipated by Farley et al. (U.S. Patent Application Number 2002/0078381).

7. Regarding claims 1, 15, and 29, Farley discloses a computerized method comprising:

monitoring a peer-to-peer network for suspicious activity based on patterns of activity (Farley, paragraphs 16, 56, and 66, Farley discloses monitoring a peer-to-peer network for predefined patterns); and

performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network (Farley, Paragraph 16,)

Claims 15 and 29 include a computer-readable medium and system performing the same functionality as claim 1 and are therefore are rejected under the same prior art as being substantially similar.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Welch, Jr. et al. (U.S. Patent Number 5,862,335) in view of Conklin et al. (U.S. Patent Number 5,991,881).

8. Regarding claims 1, 15, and 29, Welch discloses a computerized method comprising:

monitoring a peer-to-peer network for suspicious activity based on patterns of activity (Welch, col. 1, lines 45-55, col. 2, lines 35-43); and

However, Welch does not explicitly state performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network.

In an analogous art, Conklin discloses a network surveillance system that monitors network traffic and monitoring against predefined patterns and performing an action if one is come across (Conklin, col. 4, lines 45-67).

Therefore, it would have been obvious to one in the ordinary skill in the art at the time of the invention to incorporate the teachings of monitoring against predefined patterns into Welch to identify unauthorized activities such as methods and systems used by hackers to intrude into computer networks (Conklin, col. 1, lines 10-15). Claims 15 and 29 include a computer-readable medium and system performing the same functionality as claim 1 and are therefore are rejected under the same prior art as being substantially similar.

9. Regarding claims 2, 16, and 30, Welch and Conklin disclose the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein monitoring a peer-to-peer network comprises:

evaluating network traffic among peers in the peer-to-peer network (Conklin, col. 3, lines 60-65, Conklin discloses evaluating all traffic in its entirety).

10. Regarding claims 3, 17, and 31, Welch and Conklin disclose the limitations, substantially as claimed, as described in claims 1, 15, and 29, including evaluating a change in shared data on a peer in the peer-to-peer network (Welch, col. 2, lines 45-55,

Welch discloses monitoring file transfers and logical connections by determining the context of each packet in relationship to earlier packets exchanged between two stations).

11. Regarding claims 4, 18, and 32, Welch and Conklin disclose the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein a pattern of activity is defined in terms of a threshold value of network traffic in the peer-to-peer network (Conklin, col. 4 line 45 through col. 5, line10, Conklin discloses checking against patterns of normal tolerance and measured characteristics).

12. Regarding claims 5 19, and 33, Welch and Conklin disclose the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network that uses a specific protocol (Conklin, col. 4, lines 45-55, Conklin discloses patterns of activity defined in terms of network traffic).

13. Regarding claims 6, 20, and 34, Welch and Conklin disclose the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network that accesses shared data on a peer (Conklin, col. 4, lines 45-55).

14. Regarding claims 7, 21, and 35, Welch and Conklin disclose the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network having a foreign address (Conklin, col. 5, lines 25-35).

15. Regarding claims 8, 22, and 36, Welch and Conklin disclose the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein a pattern of activity is defined in terms of a configuration of shared data on a peer (Welch, col. 2, lines 45-55, Conklin, col. 4, lines 45-55).

16. Regarding claims 9, 23, and 37, Welch and Conklin disclose the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein the action comprises logging information about the particular pattern (Conklin, col. 5, lines 33-35).

17. Regarding claims 10, 24, and 38, Welch and Conklin disclose the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein the action comprises sending an alert about the particular pattern (Conklin, col. 5, lines 30-33).

18. Regarding claims 11, 25, and 39, Welch and Conklin disclose the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein the patterns of activity are local to a peer in the peer-to-peer network (Welch, col. 10, lines 5-10).

19. Regarding claims 12, 26, and 40, Welch and Conklin disclose the limitations, substantially as claimed, as described in claims 1, 15, and 29, including wherein the patterns of activity are global to the peer-to-peer network (Conklin, col. 2, lines 50-58).

20. Regarding claims 13, 27, and 43, Welch and Conklin disclose the limitations, substantially as claimed, as described in claims 1, 15, and 29, including obtaining a set of rules specifying the patterns of activity and associated actions (Conklin, col. 4, lines 45-55).

21. Regarding claims 14, 28, and 44, Welch and Conklin disclose the limitations, substantially as claimed, as described in claims 1, 15, and 29, including refreshing the set of rules when the set of rules changes (Conklin, col. 4, lines 48-52).

22. Regarding claim 41, Welch and Conklin disclose the limitations, substantially as claimed, as described in claim 40, including wherein the system is a border firewall (Conklin, col. 4, lines 45-55, Conklin discloses a set of predefined rules that make up the adaptive firewall functionality).

23. Regarding claim 42, Welch and Conklin disclose the limitations, substantially as claimed, as described in claim 40, including wherein the system is a domain name server (Conklin, col. 3, lines 5-15).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to J. Bret Dennison whose telephone number is (571)272-3910. The examiner can normally be reached on M-F 8:30am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A Wiley can be reached on (571)272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JBD
Patent Examiner
AU 2143

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100